PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-143658
(43)Date of publication of application : 28.05.1999

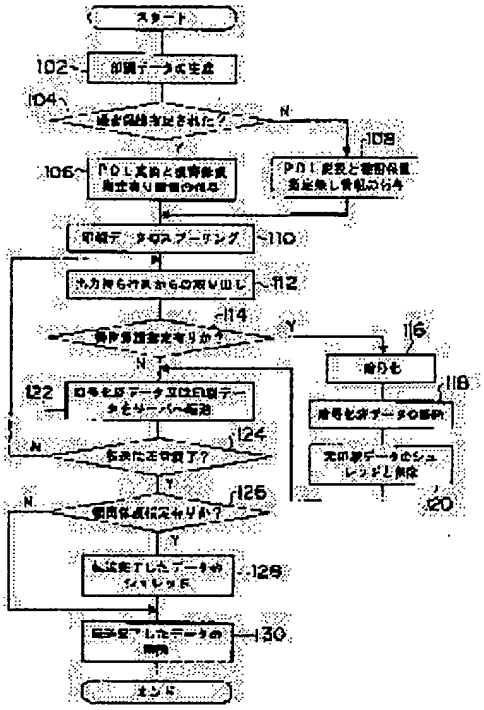
(51)Int.Cl. G06F 3/12
G06F 12/14
G06F 13/00
G06F 15/00

(21)Application number : 09-307314
(22)Date of filing : 10.11.1997

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : HIGO KAZUYOSHI

(54) NETWORK SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent printing data being a security object from being referred to by the other person and from leaking to outside and to improve the security of printing data.
SOLUTION: In a client device, printing data of the security object which becomes unnecessary after transfer completes is electronically shredded (128) and printing data which becomes unnecessary after ciphering and which is in the state of pre-ciphering (120). Thus, secret is kept on printing data after transfer completes and printing data in the state of pre-ciphering. At the same time, a printing server and a printer electronically shred printing data being the security object, which becomes unnecessary after transfer and printing complete and decoded printing data which remains when transfer and printing abnormally terminate so as to keep secret.



LEGAL STATUS

[Date of request for examination] 07.06.1999
[Date of sending the examiner's decision of rejection] 13.08.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3379411
[Date of registration] 13.12.2002
[Number of appeal against examiner's decision of rejection] 2002-17566
[Date of requesting appeal against examiner's decision of rejection] 12.09.2002
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－143658

(43)公開日　平成11年(1999)５月28日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　3/12		Ｇ０６Ｆ　3/12	Ｃ
12/14	３２０	12/14	３２０Ｄ
13/00	３５１	13/00	３５１Ａ
15/00	３３０	15/00	３３０Ａ

審査請求　未請求　請求項の数５　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－307314

(22)出願日　平成９年(1997)11月10日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　肥後　和敬
埼玉県岩槻市府内３丁目７番１号　富士ゼロックス株式会社岩槻事業所内

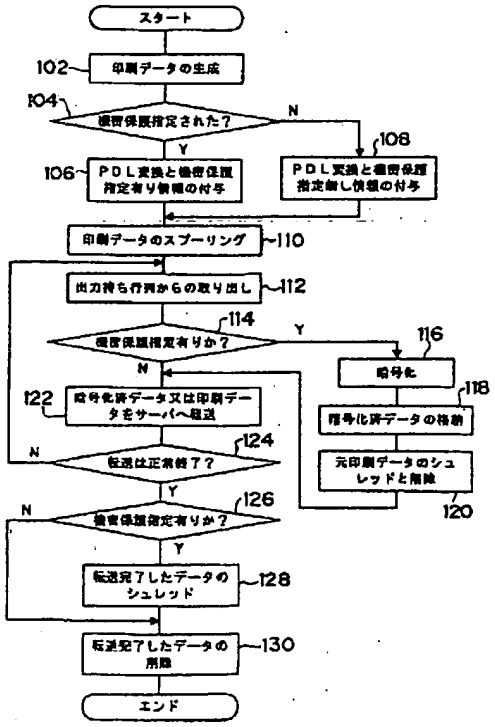
(74)代理人　弁理士　中島　淳　（外３名）

(54)【発明の名称】　ネットワークシステム

(57)【要約】

【課題】　機密保護対象の印刷データが他者により参照され外部へ漏洩することを防ぎ、印刷データの機密保護性を向上させる。

【解決手段】　クライアント装置においては、転送完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする（１２８）と共に、暗号化後に不要となった暗号化前の状態の印刷データを電子的にシュレッドする（１２０）ので、転送完了後の印刷データ及び暗号化前の状態の印刷データについて機密が保持される。これと同様に、プリントサーバ及びプリンタの各々でも、転送や印刷の完了後に不要になった機密保護対象の印刷データ、及び転送や印刷の異常終了時に残存した復号された印刷データを電子的にシュレッドして、機密を保持する。



1

【特許請求の範囲】

【請求項１】　ネットワークを介して互いに接続されたクライアント装置、プリントサーバ及びプリンタを含んで構成され、前記クライアント装置から転送された印刷データが前記プリントサーバで一旦受信された後プリンタへ転送され、又は前記クライアント装置からの印刷データが前記プリンタへ直接転送され、該プリンタが受信した印刷データを印刷するネットワークシステムであって、

前記クライアント装置は、

機密保護対象とする印刷データを指定するための機密保護指定手段と、

前記機密保護指定手段により機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する情報付加手段と、

前記属性情報付加手段により機密属性情報が付加された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第１の加工手段と、

を有し、

前記プリンタ及び前記プリントサーバの各々は、

受信した印刷データに機密属性情報が付加されているか否かを判定する判定手段と、

前記判定手段により機密属性情報が付加されていると判定された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第２の加工手段と、

を有するネットワークシステム。

【請求項２】　前記第１の加工手段及び前記第２の加工手段の少なくとも一方は、前記機密属性情報が付加された印刷データの転送完了後又は印刷完了後に、該印刷データを判読不能なデータに加工することを特徴とする請求項１記載のネットワークシステム。

【請求項３】　前記クライアント装置は、

前記印刷データを暗号化する暗号化手段をさらに有し、

前記第１の加工手段は、前記暗号化手段による印刷データの暗号化が行われた後、暗号化前の状態で残存した印刷データを判読不能なデータに加工し、

前記プリンタ及び前記プリントサーバの少なくとも一方は、前記暗号化手段により暗号化された印刷データを復号する復号化手段をさらに有し、

前記第２の加工手段は、前記復号化手段により復号された印刷データの転送完了後又は印刷完了後に、該復号された印刷データを判読不能なデータに加工する、

ことを特徴とする請求項１記載のネットワークシステム。

【請求項４】　前記第１の加工手段及び前記第２の加工手段の少なくとも一方は、前記機密属性情報が付加された印刷データの削除が指示された場合に、該印刷データを判読不能なデータに加工することを特徴とする請求項１記載のネットワークシステム。

【請求項５】　端末装置及び前記端末装置から転送されてきた印刷データを印刷するプリンタを含んで構成されたネットワークシステムであって、

前記端末装置は、

機密保護対象とする印刷データを指定するための機密保護指定手段と、

前記機密保護指定手段により機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する情報付加手段と、

前記属性情報付加手段により機密属性情報が付加された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第１の加工手段と、

を有し、

前記プリンタは、

受信した印刷データに機密属性情報が付加されているか否かを判定する判定手段と、

前記判定手段により機密属性情報が付加されていると判定された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第２の加工手段と、

を有するネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークシステムに係り、より詳しくは、クライアント装置又は端末装置からの印刷データを、ネットワークを介してプリンタへ転送し、プリンタで該印刷データを印刷するネットワークシステムに関する。

【０００２】

【従来の技術】従来より、プリントシステムにおける機密保護方式として、印刷データ送信元であるクライアント装置が、該印刷データの取り出しを許可するパスワード情報を印刷データに付与してプリンタあるいはプリントサーバへ転送し、プリンタあるいはプリントサーバが、受信した印刷ジョブを一旦保留・保管した後、操作者から正規のパスワード（＝印刷データに付与されたパスワード情報に合致するパスワード）が入力された場合に印刷データをメモリから取り出し、印刷データの参照や印刷を実行する技術が知られている（特開平８－３１４６５９号公報参照）。

【０００３】ところが、上記の技術は、プリンタあるいはプリントサーバにおいて、印刷データの取り出しが、正規のパスワードが入力されるまで抑止されるというだけであり、何ら暗号化等が施されていない印刷データが伝送路上を流れるという点で機密保護方式としては不十分であった。

【０００４】これを改善するものとして、送信元であるクライアント装置が印刷データを暗号化し、暗号化された印刷データをプリンタあるいはプリントサーバへ転送し、これを受信したプリンタあるいはプリントサーバが復号して印刷データの参照や印刷を実現する技術が提案されている。この方式では、暗号化された印刷データを

伝送路上に流すことにより、伝送路上での印刷データの漏洩・判読を防止している。

【０００５】このような暗号化技術と上記特開平８－３１４６５９号公報記載の技術とを併せて利用することにより、機密保護性はかなり高まったといえる。

【０００６】しかしながら、これらの機密保護方式においては、暗号化や復号化を行った後に不要となった印刷データの機密保護については考慮されておらず、この不要となった印刷データがクライアント装置、プリンタ、プリントサーバの各々に内蔵された記憶装置（例えば、磁気ディスク装置等）に判読可能な状態で放置されてしまう。

【０００７】即ち、通常利用されるＯＳ（Real Time Monitor 等も含むOperating System）提供のファイルシステムでは、データの削除は、例えばファイルコントロールブロック内の削除ビットをオンにする等のデータ管理情報の変更操作による見かけ上での削除にすぎず、実際に削除対象のデータがＮＵＬＬデータ（Ｘ’００’）でクリアされる等の処理が施されるわけではない。

【０００８】したがって、暗号化前の印刷データ及び復号化後の印刷データの中身は、他のファイルの新規作成や更新等の保存処理によりその記憶領域が他のデータで上書きされるまで、削除前と同じ状態で記憶装置上に存在し続けることとなる。

【０００９】このため、通常用いられるファイル復旧ツールやディスクダンプツール等を利用すれば、機密保護対象の印刷データであっても参照できてしまう、といった問題があった。

【００１０】

【発明が解決しようとする課題】本発明は、上記問題点を解消するために成されたものであり、機密保護対象の印刷データが他者により参照され外部へ漏洩することを防ぎ、印刷データの機密保護性を向上させることができるネットワークシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するために、本発明に係るネットワークシステムは、ネットワークを介して互いに接続されたクライアント装置、プリントサーバ及びプリンタを含んで構成され、前記クライアント装置から転送された印刷データが前記プリントサーバで一旦受信された後プリンタへ転送され、又は前記クライアント装置からの印刷データが前記プリンタへ直接転送され、該プリンタが受信した印刷データを印刷するネットワークシステムであって、前記クライアント装置は、機密保護対象とする印刷データを指定するための機密保護指定手段と、前記機密保護指定手段により機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する情報付加手段と、前記属性情報付加手段により機密属性情報が付加された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第１の加工手段と、を有し、前記プリンタ及び前記プリントサーバの各々は、受信した印刷データに機密属性情報が付加されているか否かを判定する判定手段と、前記判定手段により機密属性情報が付加されていると判定された印刷データを、該印刷データが不要となった時点で判読不能なデータに加工する第２の加工手段と、を有することを特徴とする。

【００１２】本発明に係るネットワークシステムは、ネットワークを介して互いに接続されたクライアント装置、プリンタ及びプリントサーバを含んで構成されている。クライアント装置から転送された印刷データは、プリントサーバで一旦受信された後プリンタへ転送されるか、又はプリンタへ直接転送され、該プリンタにより印刷される。

【００１３】このようなネットワークシステムにおいて、クライアント装置のユーザが機密保護指定手段により、機密保護対象とする印刷データを指定すると、情報付加手段は、該機密保護対象として指定された印刷データに、機密保護対象を示す機密属性情報を付加する。この機密属性情報としては、例えば、１ビットで構成されるフラグ（機密保護対象の場合「１」、機密保護対象でない場合「０」など）を用いることができる。

【００１４】この機密属性情報が付加された印刷データは、前述したように、プリントサーバで一旦受信された後プリンタへ転送されるか又はプリンタへ直接転送されるが、該印刷データが不要となった時点（例えば、該印刷データの転送完了後や、印刷取消しや印刷データの転送取消し等により印刷データの削除がユーザにより指示されたとき等）で、第１の加工手段により判読不能なデータに加工される。

【００１５】なお、判読不能なデータへの加工方法としては、ＮＵＬＬデータによるクリア、乱数によるスクランブル、各種の暗号化等を採用することができる。

【００１６】これにより、クライアント装置において、不要となった機密保護対象の印刷データが該クライアント装置内のメモリに判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【００１７】プリントサーバは上記機密属性情報が付加された印刷データを一旦受信した後、プリンタへ転送するが、このプリントサーバにおいて、判定手段が、受信した印刷データに機密属性情報が付加されているか否かを判定する。そして、第２の加工手段は、この判定結果により機密属性情報が付加されていると判定された印刷データ（即ち、機密保護対象として指定された印刷データ）を、該印刷データが不要となった時点（例えば、プリンタへの該印刷データの転送完了後や、印刷取消しや印刷データの転送取消し等により印刷データの削除がユーザにより指示されたとき等）で判読不能なデータに加工する。

【００４３】ここで、印刷データが機密保護指定されていなければ、後述するステップ１２２へ進み、印刷データが機密保護指定されておれば、ステップ１１６へ進む。このステップ１１６では、暗号化制御部１７によって印刷データの暗号化を行い、次のステップ１１８で暗号化済の印刷データを、スプーリング制御部１５によって記憶装置１８に格納する。さらに、次のステップ１２０では、暗号化によって不要となった暗号化前の印刷データを電子的にシュレッドした後削除する。

【００４４】次のステップ１２２では、暗号化済の印刷データ又は機密保護指定されていない印刷データを、伝送制御部１２の制御に基づいて、伝送Ｉ／Ｆ１１を経由してプリントサーバ２０へ転送する。

【００４５】ここでの転送が何らかの理由により正常に完了しなかった場合、スプーリング制御部１５によって印刷データは記憶装置１８に保持される。そして、ステップ１１２へ戻り、ステップ１１２～１２２の処理を再実行する。

【００４６】一方、ステップ１２２での転送が正常終了した場合は、ステップ１２６へ進み、不要となった転送済の印刷データが機密保護指定されているか否かを、該印刷データに付与された属性情報に基づいて判定する。

【００４７】ここで、印刷データが機密保護指定されていなければ、該印刷データの削除のみを行う（ステップ１３０）。一方、印刷データが機密保護指定されている場合には、該印刷データをデータ加工部１９によって電子的にシュレッドした（ステップ１２８）後、削除する（ステップ１３０）。

【００４８】以上のように、クライアント装置１０においては、転送完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする（図２のステップ１２８）ので、転送完了後の印刷データについて機密が保持される。また、暗号化後に不要となった暗号化前の状態の印刷データを電子的にシュレッドする（図２のステップ１２０）ので、暗号化前の状態の印刷データについて機密が保持される。

【００４９】プリントサーバ２０においては図３の制御ルーチンが実行される。図３のステップ２０２では、伝送制御部２２の制御に基づいて、クライアント装置１０からの属性情報付きの印刷データ（即ち、暗号化済の印刷データ又は機密保護指定されていない印刷データ）を受信し、次のステップ２０４では受信した印刷データをスプーリング制御部２４によって記憶装置２６に格納する。

【００５０】そして、次のステップ２０６では、目的とするプリンタ３０がデータの受け入れ準備可能であるか否かをプリンタ管理部２９によって判定する。ここで、プリンタ３０がデータの受け入れ準備可能と判定された時点で、ステップ２０８へ進み、属性情報付きの印刷データをスプーリング制御部２４の待ち行列制御に従って記憶装置２６から取り出す。

【００５１】次のステップ２１０では、印刷データが機密保護指定されているか否かを、該印刷データに付与された属性情報に基づいて判定する。ここで、印刷データが機密保護指定されていなければ、後述するステップ２１６へ進み、印刷データが機密保護指定されている場合は、ステップ２１２へ進む。ステップ２１２では、プリンタ３０が復号機能を持っているか否かをプリンタ管理部２９によって判定し、プリンタ３０が復号機能を持っていない場合のみ、ステップ２１４へ進み、復号化制御部２５によって各種暗号化に対応した復号処理を印刷データに対し実行し、復号された印刷データ（復号化済の印刷データ）を記憶装置２６に格納する。

【００５２】次のステップ２１６では、ステップ２１４で得られた復号化済の印刷データ又は機密保護指定されていない印刷データを、伝送制御部２２の制御に基づいて伝送Ｉ／Ｆ２１を経由してプリンタ装置３０へ転送する。

【００５３】ここでの転送が何らかの理由により正常に完了しなかった場合、スプーリング制御部２４によって印刷データは記憶装置２６に保持されるが、ステップ２２０で、該印刷データが機密保護指定されているか否かを判定部２７によって判定し、機密保護指定されている場合のみステップ２２２へ進み、該印刷データ（ここでは復号化済の印刷データ）をデータ加工部２８によって電子的にシュレッドして削除する。

【００５４】その後、ステップ２０８へ戻り、ステップ２０８～２１６の処理を再実行する。

【００５５】一方、ステップ２１６での転送が正常終了した場合は、ステップ２２４へ進み、不要となった転送済の印刷データが機密保護指定されているか否かを判定部２７によって判定する。

【００５６】ここで、印刷データが機密保護指定されていなければ、該印刷データの削除のみを行う（ステップ２２８）。一方、印刷データが機密保護指定されている場合には、該印刷データをデータ加工部２８によって電子的にシュレッドした（ステップ２２６）後、削除する（ステップ２２８）。

【００５７】以上のように、プリントサーバ２０においては、転送完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする（図３のステップ２２６）ので、転送完了後の印刷データについて機密が保持される。また、転送が正常に完了しなかった場合、復号された機密保護対象の印刷データを電子的にシュレッドする（図３のステップ２２２）ので、復号された状態の印刷データについて機密が保持される。

【００５８】プリンタ３０においては図４の制御ルーチンが実行される。図４のステップ３０２では、伝送制御部３２によって、プリントサーバ２０からの属性情報付きの印刷データ（即ち、暗号化済の印刷データ、復号化

済の印刷データ、機密保護指定されていない印刷データの何れか）を受信し、次のステップ３０４では受信した印刷データをスプーリング制御部３５の制御に基づいて記憶装置３９に格納する。

【００５９】そして、次のステップ３０６では、転写部３８が転写可能状態となったか否かを判定する。ここで、転写部３８が転写可能状態となった時点で、ステップ３０８へ進み、属性情報付きの印刷データをスプーリング制御部３５の待ち行列制御に従って記憶装置３９から取り出す。

【００６０】次のステップ３１０では、印刷データが機密保護指定されているか否かを、該印刷データに付与された属性情報に基づいて判定する。ここで、印刷データが機密保護指定されていなければ、後述するステップ３１６へ進み、印刷データが機密保護指定されている場合は、ステップ３１２へ進む。ステップ３１２では、該印刷データが暗号化された状態の印刷データ（即ち、暗号化済の印刷データ）であるか否かを判定し、該印刷データが暗号化された状態の印刷データである場合のみ、ステップ３１４へ進み、復号化制御部３４によって各種暗号化に対応した復号処理を印刷データに対し実行し、復号された印刷データ（復号化済の印刷データ）を記憶装置３９に格納する。

【００６１】次のステップ３１６では、上記復号された印刷データ、プリントサーバ２０で既に復号されていた印刷データ、機密保護指定されていない印刷データに対して、ラスタライザ３６によりラスタライズ処理が施され、ラスタイメージに展開される。そして、次のステップ３１８では、該ラスタイメージを印刷制御部３７の制御に基づいて転写部３８に転送し用紙に転写することで、印刷処理を行う。

【００６２】ここでの印刷処理が何らかの理由により正常に終了しなかった場合、スプーリング制御部３５の制御によって印刷データは記憶装置３９に保持されるが、ステップ３２２で、該印刷データが機密保護指定されているか否かを判定部３Ａによって判定し、機密保護指定されている場合のみステップ３２４へ進み、該印刷データ（ここでは復号化済の印刷データ）をデータ加工部３Ｂによって電子的にシュレッドして削除する。

【００６３】その後、ステップ３０８へ戻り、ステップ３０８～３１８の処理を再実行する。

【００６４】一方、ステップ３１８での印刷処理が正常終了した場合は、ステップ３２６へ進み、不要となった印刷済の印刷データが機密保護指定されているか否かを判定部３Ａによって判定する。

【００６５】ここで、印刷データが機密保護指定されていなければ、該印刷データの削除のみを行う（ステップ３３０）。一方、印刷データが機密保護指定されている場合には、該印刷データをデータ加工部３Ｂによって電子的にシュレッドした（ステップ３２８）後、削除する（ステップ３３０）。

【００６６】以上のように、プリンタ３０においては、印刷完了後に不要になった機密保護対象の印刷データを電子的にシュレッドする（図４のステップ３２８）ので、印刷完了後の印刷データについて機密が保持される。また、印刷が正常に完了しなかった場合、復号された機密保護対象の印刷データを電子的にシュレッドする（図４のステップ３２４）ので、復号された状態の印刷データについて機密が保持される。

【００６７】ところで、クライアント装置１０のユーザは、前述した図２の制御ルーチンの任意の処理時点で、印刷処理の取消しや転送の取消しといった印刷データを削除する指示をクライアント装置１０に対して操作制御部１６を通じて指示可能である。即ち、クライアント装置１０のユーザにより印刷データの削除指示が行われると、クライアント装置１０において図５の処理ルーチンが割り込み処理される。まず、印刷データの削除指示を受け取ったスプーリング制御部１５は、該印刷データが機密保護指定されているか否かをチェックし（ステップ４０２）、機密保護指定されていなければ、該印刷データの削除のみを行う（ステップ４０６）。一方、印刷データが機密保護指定されている場合は、該印刷データをデータ加工部１９によって電子的にシュレッドして（ステップ４０４）、削除する（ステップ４０６）。

【００６８】このように、機密保護指定された印刷データに対して削除指示が行われた（印刷の取消しや転送の取消しが指示された）場合、該印刷データは直ちに電子的にシュレッドされるので、不要となった機密保護対象の印刷データが記憶装置１８に判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【００６９】なお、上記のような機密保護指定の印刷データに対する削除指示時の割り込み処理（図５）は、クライアント装置１０だけでなく、プリントサーバ２０及びプリンタ３０においても実行される。即ち、プリントサーバ２０のユーザが、印刷処理の取消しや転送の取消しといった印刷データ削除指示を、操作制御部２３を通じて行えば、図５の処理ルーチンが割り込み処理され、機密保護対象の印刷データについてはデータ加工部２８によって直ちに電子的にシュレッドされる。また、プリンタ３０のユーザが、印刷処理の取消しや転送の取消しといった印刷データ削除指示を、操作制御部３３を通じて行えば、図５の処理ルーチンが割り込み処理され、機密保護対象の印刷データについてはデータ加工部３Ｂによって直ちに電子的にシュレッドされる。

【００７０】このようにして、プリントサーバ２０やプリンタ３０においても、不要となった機密保護対象の印刷データが記憶装置に判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【００７１】以上説明した実施形態によれば、クライアント装置１０のアプリケーション１３が印刷データを生成してから、プリンタ３０が該印刷データを印刷完了するまでの一連の印刷処理に関わるクライアント装置１０、プリントサーバ２０、プリンタ３０の各々において、機密保護指定の印刷データは不要になった時点で直ちに電子的にシュレッドされるので、意図しない他者により印刷データが参照される可能性がなくなるため、印刷システムとして一貫した機密保護を保つことができる。

【００７２】なお、本実施形態においては、プリントサーバ２０に復号化制御部２５を設けているが、この復号化制御部２５は、プリンタ３０が旧来のプリンタのように復号化機構を備えていない場合にのみ必要となるものである。プリントサーバ２０の復号化制御部２５によって、暗号化された印刷データを復号し、復号された印刷データを、伝送媒体４１を介してプリンタ３０へ転送する場合、判読可能な印刷データが伝送媒体４１を流れてしまうため、機密保護上は本来望ましくないものである。但し、実際の利用現場では、様々な仕様を有する各種のプリンタを混在利用するケースが多いと想定されるため、上記実施形態では、プリントサーバ２０に復号化制御部２５を設け、復号化機構を備えていないプリンタから印刷データを印刷する場合でも対応可能な構成例を説明した。

【００７３】また、上記実施形態では、クライアント装置１０で生成した印刷データを、プリントサーバ２０を経由してプリンタ３０へ転送して印刷する処理形態に本発明を適用した例を示したが、クライアント装置１０からプリントサーバ２０に対し印刷要求のみを行い、印刷データについてはクライアント装置１０からプリンタ３０へ直接転送して印刷する処理形態についても、本発明は適用可能である。もちろん、図６に示すように端末装置７０とプリンタ８０とがローカル接続されたネットワークシステム９０についても、本発明が適用可能であることは言う迄もない。

【００７４】また、印刷データを暗号化した状態で装置間を転送しない場合でも、クライアント装置やプリントサーバでは転送完了後に、プリンタでは印刷完了後に不要となった印刷データを電子的にシュレッドすることにより、印刷データの機密性向上が図れる。また、ユーザにより印刷データの削除指示が行われた時に、直ちに印刷データを電子的にシュレッドすることにより、印刷データの機密性向上が図れる。

【００７５】

【発明の効果】以上説明したように、本発明によれば、機密保護対象として指定された印刷データは、クライアント装置、サーバ及びプリンタの各々において、該印刷データが不要となった時点で、判読不能なデータに加工されるので、不要となった機密保護対象の印刷データが装置内のメモリに判読可能な状態で残存し、意図しない他者により参照され、外部へ漏洩してしまうことを未然に防ぐことができる。

【図面の簡単な説明】

【図１】発明の実施形態におけるネットワークシステムの概略構成図である。

【図２】クライアント装置において実行される制御ルーチンを示す流れ図である。

【図３】プリントサーバにおいて実行される制御ルーチンを示す流れ図である。

【図４】プリンタにおいて実行される制御ルーチンを示す流れ図である。

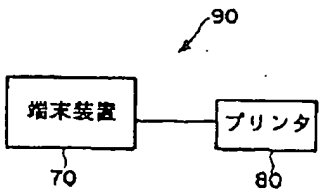
【図５】印刷データの削除指示により実行される割り込み処理ルーチンを示す流れ図である。

【図６】本発明を適用可能な他のネットワークシステムの概略構成図である。

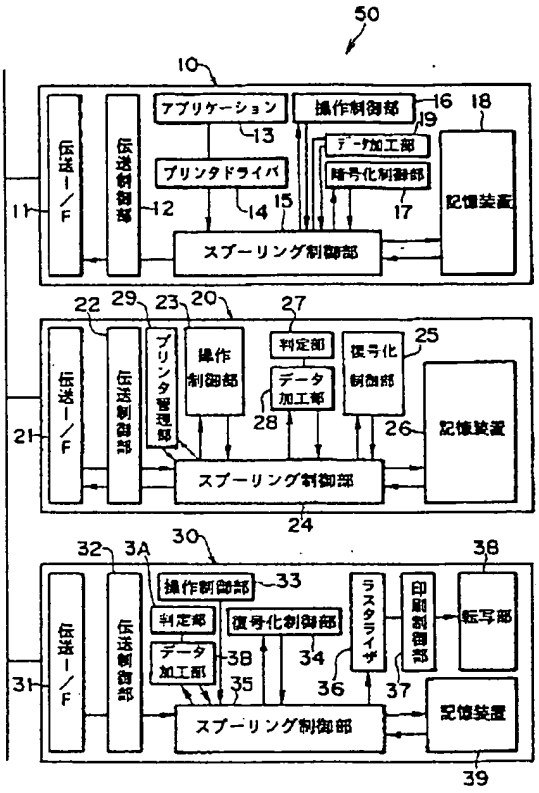
【符号の説明】

１０　クライアント装置
１５、２４、３５　スプーリング制御部
１６　操作制御部（機密保護指定手段）
１７　暗号化制御部（暗号化手段）
１８、２６、３９　記憶装置
１９　データ加工部（第１の加工手段、情報付加手段）
２０　プリントサーバ
２５、３４　復号化制御部（復号化手段）
２７、３Ａ　判定部（判定手段）
２８、３Ｂ　データ加工部（第２の加工手段）
３０　プリンタ
４１　伝送媒体
５０　ネットワークシステム

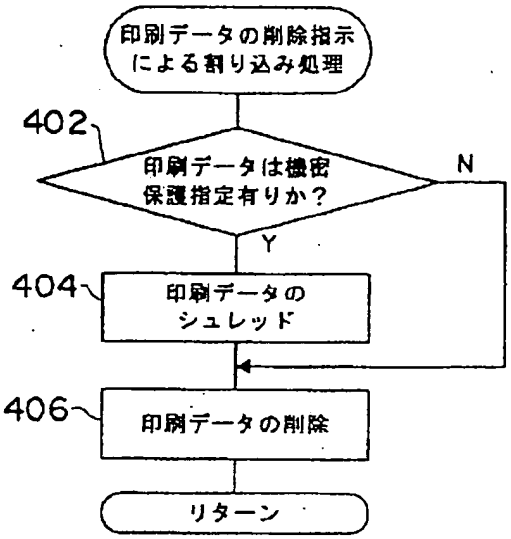
【図６】



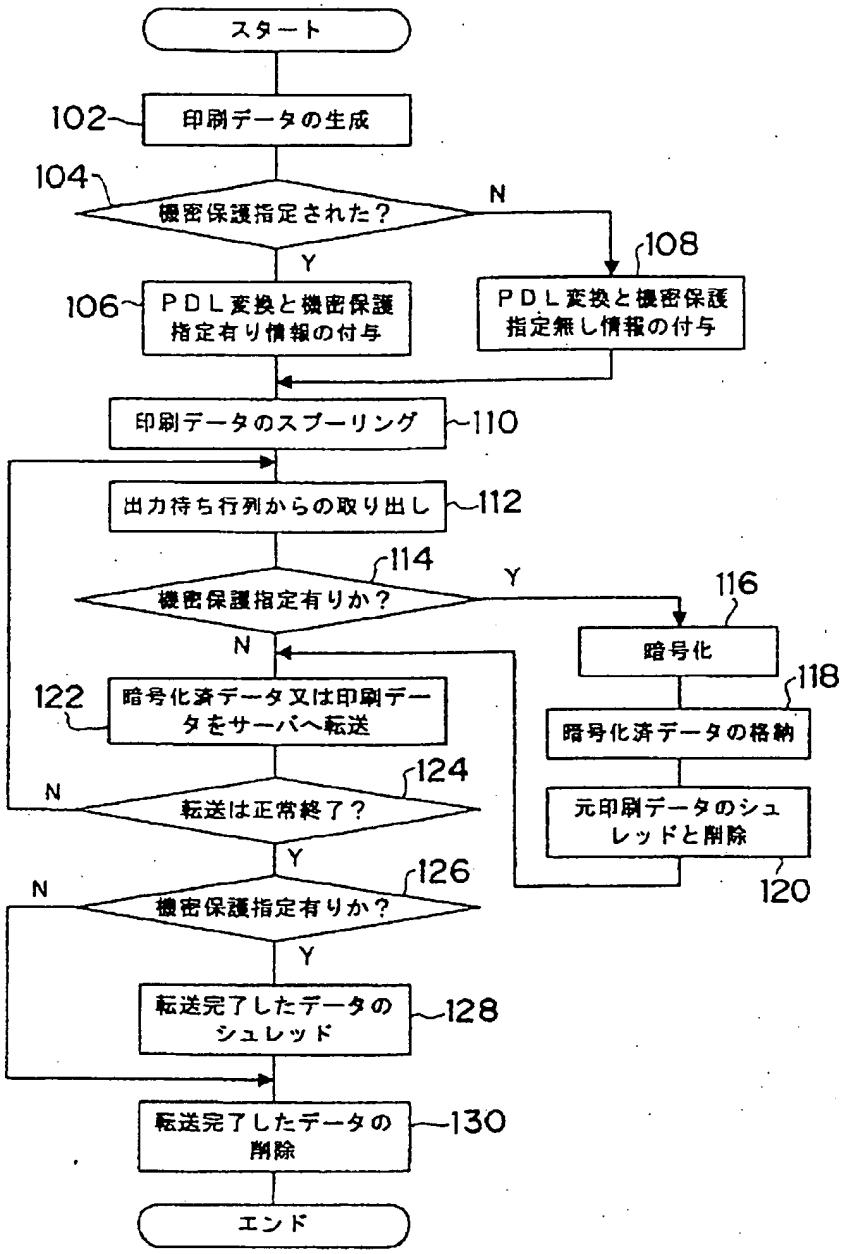
【図１】


50
10
アプリケーション
13
操作制御部
16
18
19
データ加工部
暗号化制御部
プリンタドライバ
12
14
15
17
記憶装置
スプーリング制御部
伝送I／F
伝送制御部
11
22
29
23
20
27
プリンタ管理部
操作制御部
判定部
データ加工部
復号化制御部
25
28
26
21
24
30
32
3A
33
38
復号化制御部
ラスタライザ
印刷制御部
転写部
34
36
37
31
35
39

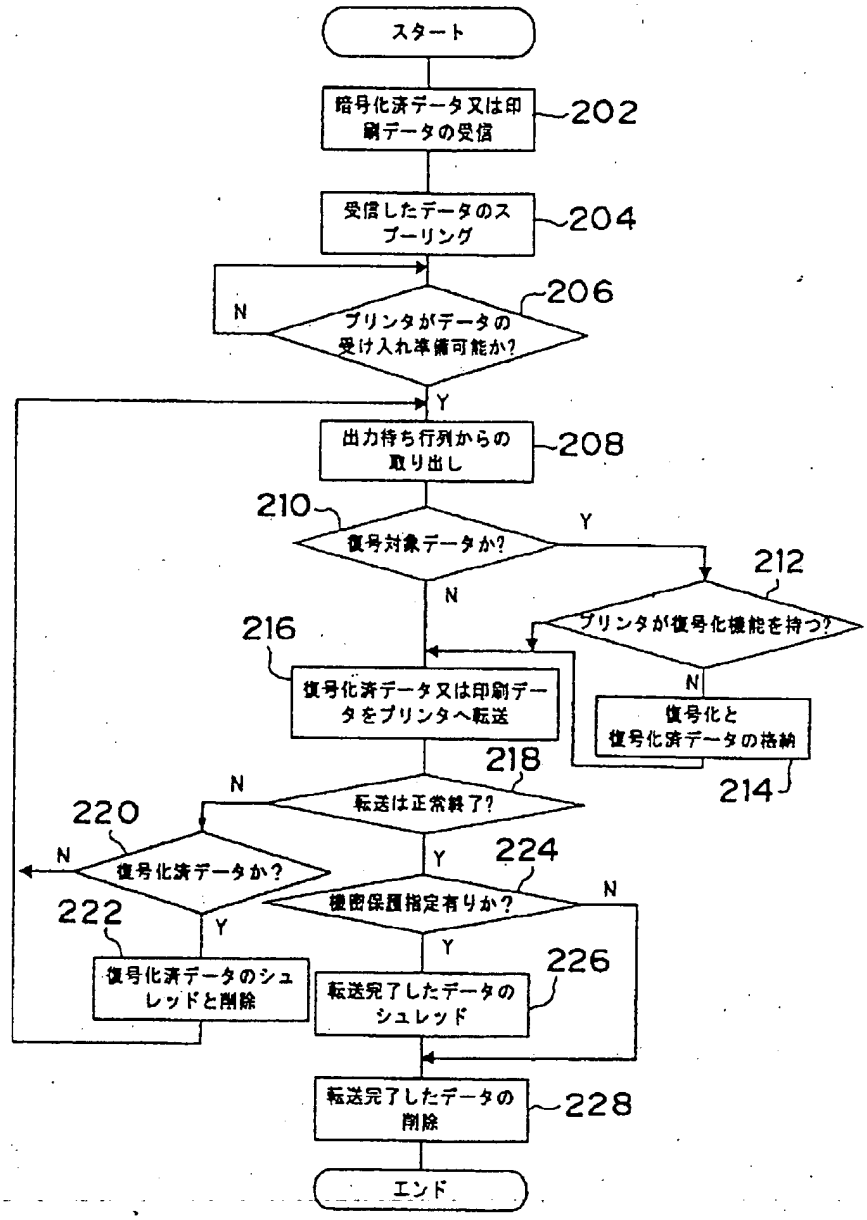
【図５】


印刷データの削除指示による割り込み処理
402
印刷データは機密保護指定有りか？
N
Y
404
印刷データのシュレッド
406
印刷データの削除
リターン

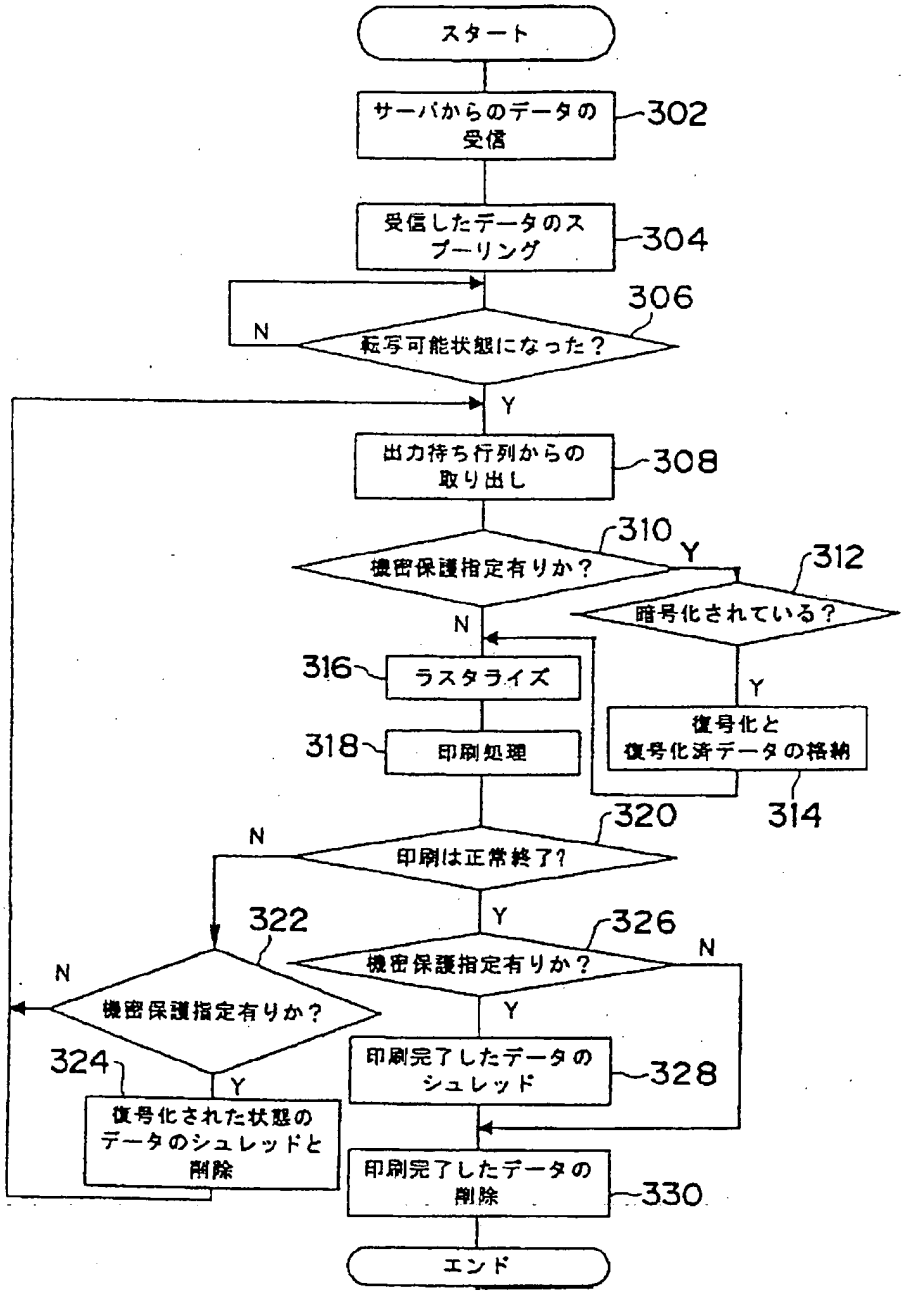
【図２】


スタート
102
印刷データの生成
104
機密保護指定された？
N
Y
108
PDL変換と機密保護指定無し情報の付与
106
PDL変換と機密保護指定有り情報の付与
印刷データのスプーリング
110
出力待ち行列からの取り出し
112
114
機密保護指定有りか？
Y
116
暗号化
N
118
暗号化済データの格納
122
暗号化済データ又は印刷データをサーバへ転送
124
転送は正常終了？
N
Y
元印刷データのシュレッドと削除
120
126
機密保護指定有りか？
N
Y
転送完了したデータのシュレッド
128
転送完了したデータの削除
130
エンド

【図３】


スタート
暗号化済データ又は印刷データの受信
202
受信したデータのスプーリング
204
プリンタがデータの受け入れ準備可能か?
206
N
Y
出力待ち行列からの取り出し
208
210
復号対象データか?
Y
N
212
プリンタが復号化機能を持つ?
N
復号化と復号化済データの格納
214
216
復号化済データ又は印刷データをプリンタへ転送
218
転送は正常終了?
N
Y
220
復号化済データか?
N
Y
222
復号化済データのシュレッドと削除
224
機密保護指定有りか?
N
Y
226
転送完了したデータのシュレッド
転送完了したデータの削除
228
エンド

【図４】


スタート
サーバからのデータの受信
302
受信したデータのスプーリング
304
306
転写可能状態になった？
N
Y
出力待ち行列からの取り出し
308
310
機密保護指定有りか？
Y
312
暗号化されている？
N
316
ラスタライズ
318
印刷処理
Y
復号化と復号化済データの格納
314
320
印刷は正常終了？
N
Y
322
機密保護指定有りか？
N
326
機密保護指定有りか？
N
Y
324
Y
復号化された状態のデータのシュレッドと削除
印刷完了したデータのシュレッド
328
印刷完了したデータの削除
330
エンド